REMARKS

In response to the Examiner's non-final Office Action of January 16, 2004 the Applicant respectfully submits the following remarks against the Examiner's rejections of claims 1 to 20 under 35 U.S.C. §103(a) over Sony Corporation (EP 0817420) in view of Herbert et al. (USP 6,023,509), without amendment to the pending claims.

Regarding independent claims 1 and 11, a validation protocol for determining whether or not an untrusted authentication chip is valid and a system which performs this protocol are provided. The protocol includes the steps of:

generating a secret random number and calculating a signature for the random number using a signature function, in a trusted authentication chip;

encrypting the random number and the signature by a symmetric encryption function using a first key, in the trusted authentication chip;

passing the encrypted random number and signature from the trusted authentication chip to an untrusted authentication chip;

decrypting the encrypted random number and signature with a symmetric decryption function using the first key, in the untrusted authentication chip;

calculating a signature for the decrypted random number using the signature function, in the untrusted authentication chip;

comparing the signature calculated in the untrusted authentication chip with the signature decrypted;

in the event that the two signatures match, encrypting the decrypted random number by the symmetric encryption function using a second key and returning it to the trusted authentication chip;

encrypting the random number by the symmetric encryption function using the second key, in the trusted authentication chip;

comparing the two random numbers encrypted using the second key, in the trusted authentication chip;

in the event that the two random numbers encrypted using the second key match, considering the untrusted authentication chip to be valid; and

otherwise considering the untrusted authentication chip to be invalid.

The Examiner contends that Sony discloses all of the above steps of claims 1 and 11 in their authentication method except the calculation and comparison of a digital signature. The Examiner then contends that Herbert discloses the use of such digital signatures and as such it would have been obvious to use them in the authentication method of Sony. Applicant respectfully disagrees for at least the following reasons.

Herbert discloses that the digital signature is encrypted by the originator using its private key and the encrypted signature is sent to the recipient together with the originator's public key. The recipient then decrypts the encrypted digital signature using the public key. Thus, if this process was to be incorporated into the authentication method of Sony (disclosed at col. 8, line 12 to col. 10, line 39) as suggested by the Examiner, then the R/W (1) would use the key K_B to encrypt the digital signature and would send this encrypted signature to the IC card (2) with its public key. The IC card would then use the public key of the R/W to decrypt the encrypted signature, not the key K_B.

This process would be clearly different than that recited in claims 1 and 11, because in claims 1 and 11 the encrypted signature is decrypted by the untrusted chip using the same (secret) key that was used to encrypt the signature by the trusted chip, and not a separate (public) key.

Further, Herbert does not teach or suggest for the recipient to independently form the signature to be compared with the decrypted signature. Rather, Herbert discloses that the recipient generates a hash value from the data from the originator and compares this with the hash value recovered from the decrypted signature. Therefore, in the Examiner's modified authentication method of Sony, the IC card would not calculate a signature for the decrypted random number and compare this to the decrypted signature from the R/W, as in claims 1 and 11.

Further still, even if the authentication method of Sony was to be modified as contended by the Examiner, differences would still remain from the protocol and system of claims 1 and 11. This is because, in Sony the R/W decrypts the encrypted random number RA using the key K_A and compares this to the originally generated random number R_A (see col. 10, lines 21-35), whereas in claims 1 and 11, the trusted chip encrypts the random number using the second key and compares this to the encrypted random number received from the untrusted chip (encrypted using the second key). Thus, it is the encrypted versions of the random number using the second key that are compared in the claimed invention, and not the random numbers themselves as in Sony. This provides heightened security in the protocol used by the claimed invention (see page 52, lines 5-21 of the present specification).

Therefore, for at least the above stated reasons, it is respectfully submitted that neither Sony nor Herbert taken alone or in combination teach or suggest the subject matter of independent claims 1 and 11, and claims 2 to 10 and 12 to 20 respectively dependent therefrom.

It is respectfully submitted that all of the Examiner's rejections have been traversed. Accordingly, it is submitted that the present application is in condition for allowance and reconsideration of the present application is respectfully requested.

Very respectfully,

Applicant:

SIMON ROBERT WALMSLEY

PAUL LAPSTUN

C/o: Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia

Email: kia.silverbrook@silverbrookresearch.com
Telephone: +612 9818 6633
Facsimile: +61 2 9555 7762